13

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32, H04K 1/00

A1

(11) International Publication Number: **WO 96/37065**

(43) International Publication Date: 21 November 1996 (21.11.96)

(21) International Application Number: PCT/NO96/00117

(22) International Filing Date: 14 May 1996 (14.05.96)

(30) Priority Data:
951965 18 May 1995 (18.05.95) NO

(71) Applicant *(for all designated States except US)*: DEFA A/S [NO/NO]; Baneveien 38, Postboks 457 Nymoen, N-3601 Konsberg (NO).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: RØREN, Sigurd [NO/NO]; Runden 12, N-3647 Hvittingfoss (NO).

(74) Agent: OSLO PATENTKONTOR A/S; Postboks 7007 M, N-0306 Oslo (NO).

(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
In English translation (filed in Norwegian).

(54) Title: SECURE ONE-WAY COMMUNICATION SYSTEM

(57) Abstract

The present invention relates to a system comprising a method and a transmitter receiver arrangement for use in transmitting and receiving a message including a code which prevents unintentional use of said message. For the object of obtaining better security against unauthorized registration of said message, it is according to the invention suggested that to the message there is added a time information which in the transmitter is generated by a clock, and which in the receiver is checked by a synchronous clock. Only when the time information in the received message corresponds to the clock of the receiver the message is accepted. The timing information can be encrypted using a pseudo random code, which is transmitted together with the message.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

Secure one-way communication system

Field of the invention

The present invention relates to a system comprising a method for use in transmitting and receiving one or more signals, especially signals comprising a message and a code which prevent unintentional use of said message. The invention also relates to a transmitter and a receiver which are included in such a system.

Background of the invention

The present invention is developed for the purpose of providing a system for secure one-way communication via radio. Such a system comprises specifically a small radio transmitter which is attached to the key-ring of the user, and a radio receiver comprising control electronics mounted in the car which is at the disposal of the user. By using the radio transmitter, for example the door locks of the car are to be opened, possibly further functions of the car being triggered.

Prior art

The system of today utilizes so-called code shift to protect communication against intruders. This means that the transmitter and receiver both generate the same varying pseudo random code which is secret to the public. When the transmitter is activated, the code will be transmitted together with the command to the receiver. The receiver checks the received code with its own generated code, and by conformity the command from the transmitter will be accepted.

The problem enfaced with this solution is that if a dishonest person is able to register a command from the

transmitter when this is outside the range of the receiver, this dishonestly registered command can be used to open the car, in the time span before the authorized user once more activates the transmitter towards the receiver. Consequently, there exists a time slot wherein the system is insecure.

From DE-A-42 18 500 (Borghetto) there is known a system for remote control of for example door locks in a vehicle, especially for operating an electronic control means. There is used a transmitter for transmitting a code and a receiver checking the code prior to outputting an operating signal. In order to render difficult the copying of the code, a time variable time code has been included in the transmitter and receiver. A counter on the transmitter side has for an object to provide a time code which alters according to a specific pattern and due to counting pulses received from a control unit, and being based on synchronous pulses supplied by a clocking means.

On the receiver side there is correspondingly provided a counter which has for the object to provide an alterable time code corresponding to the time code which is provided by the counter on the transmitter side.

In other words, from the transmitter there will be transmitted a permanent identification code and a time code which is altered for example each tenth second. However, the time information according to said publication is included as a direct part of the coded message, which involves that according to the prior art there is achieved a relatively moderate security level.

Disclosure of the invention

The object of the present invention is to provide a system alleviating the previously discussed problems.

According to the present invention said problems are resolved in a method of the type as stated in the preamble, which according to the invention is characterized in that to the message and/or code there is added a time information which in the transmitter is generated by a clock, and which in the receiver is checked by a synchronous clock.

Appropriately, the invention can be realized in that there is especially used code shift by means of a pseudo random (quasi random) generated code, which is transmitted together with said message including time information.

By including said time information in a pseudo random rotating code, there is achieved a totally very high security level.

Further features and advantages of the present invention will appear from the following description as well as from the appending patent claims.

Brief description of the drawing

In the attached Fig. 1 there is illustrated a schematic principle diagram of a transmitter/receiver system wherein the present invention can find its application.

Description of embodiments

In Fig. 1 there is illustrated a key-ring comprising generally a transmitter 2, and more specifically a radio transmitter, a code generator, specifically a pseudo random code generator 3 as well as a clock 4.

In Fig. 1 there is also schematically illustrated a control unit 5, for example mounted in a car, which control unit 5 inter alia comprises a receiver 6, a pseudo random code generator 7 and a clock 8.

It is to be understood that the transmitter 2 can be of any appropriate type, not only a radio transmitter for transmitting electromagnetic waves, but also communication signals based on sound, light, IR-waves, pressure waves, etc.

The system illustrated in Fig. 1 can for example be used in alarm systems for car as well as for operation of certain functions of the car, for example opening and closing of car locks.

In other words, according to Fig. 1 there is given instructions for a system to be used for sending and receiving one or more signals, specifically signals which comprise a message or command, and a code included in said message and preventing unintentional use of said message. What is specific in said system according to Fig. 1, wherein the present invention has been included, is that in addition to said code, especially a pseudo random code, there is added a time information, preferably in said command or message. Both transmitter 2 and receiver 6 have "synchronous" clocks 4 and 8, respectively. When the command is transmitted from the transmitter 2 the time information will be included, and when the command is received in the receiver 6, the time in the command is compared to the clock 8 in the control unit 5 of the car. If the two points of time coincide, the command will be accepted by the control unit 5, and the command can then effect those functions which are assigned in said command or message.

By means of the system illustrated in Fig. 1 the command

will become obsolete after a given time interval, which can be determined by the transmitter 2 and the receiver 6. A dishonest person will consequently not be able to register a message and use the latter in order to open the car prior to the obsoletion of said message.

The clocks 4 and 8, respectively, of the transmitter 2 and the receiver 6, respectively, can be synchronized at regular intervals, and the accuracy of the synchronization will state the time interval as previously discussed. The accuracy can therefore appropriately be in the range of a second.

Patent claims

1. Method for use in transmitting and receiving one or more signals, especially signals comprising a message and a code which prevents unintentional use of said message, characterized in that to the message and/or code there is added a time information which in the transmitter is generated by a clock, and which in the receiver is checked by a synchronous clock.

2. Method as claimed in claim 1, characterized in that there is especially used code shift by means of a pseudo random (quasi random) generated code, which is transmitted together with said message including time information.

3. Method as claimed in claim 1 or 2, characterized in that when the command is received in the receiver, said command is compared with the receiver clock, and upon coincidence between said two points of time the command will be accepted.

4. Method as claimed in any of the claim 1-3, characterized in that said command becomes obsolete after a given time interval which can be determined by transmitter (2) and receiver (6).

5. Method as claimed in any of the preceding claims, characterized in that the accuracy of the synchronization is in the range of approximately 1 sec.

6. Transmitter and receiver for use in transmitting and receiving one or more signals, especially signals comprising a message and a code which prevents unintentional used of said message, characterized in that said transmitter (2) communicates with a clock (4) which generates a time

information when the transmitter transmits a message/-command, and that said receiver (6) checks the message/-command in relation to a synchronous clock communicating with said receiver (6).

7. Transmitter as claimed in claim 6, c h a r a c t e r i z e d i n that said transmitter (2) communicates with a pseudo code generator (3) which generates a pseudo random (quasi random) generated code, and that said code is transmitted together with a time information provided by said clock (4).

8. Receiver as claimed in claim 6 or 7, c h a r a c t e r i z e d i n that said receiver (6) is adapted together with said synchronous clock (8) and a pseudo random code generator (7) to comparing said received message/command and upon coincidence between said two points of time to accept said command/message.

9. Transmitter and receiver as claimed in any of the claims 6-8, c h a r a c t e r i z e d i n that said transmitter (2) and receiver (6) are adapted subsequent to a given time interval to detecting asynchronous messages/commands as obsolete.

10. Transmitter and receiver as claimed in any of the claims 6-9, c h a r a c t e r i z e d i n that said clock (4) which cooperates with said transmitter (2) and said clock (8) which cooperates with said receiver (6), have a synchronization within a time range of approximately 1 sec.

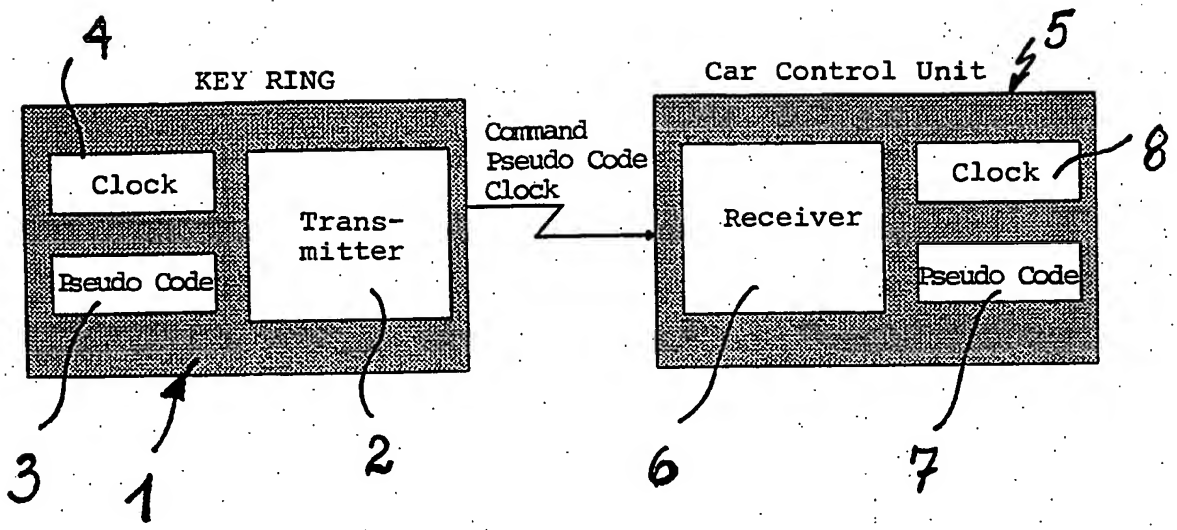
4
KEY RING
Clock
Pseudo Code
Trans-
mitter
3
1
2
Command
Pseudo Code
Clock
5
Car Control Unit
Receiver
Clock
8
Pseudo Code
6
7

FIG. 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NO 96/00117

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04L 9/32, H04K 1/00
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L, H04K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 4141766 A1 (SKULTETY, IVAN), 24 June 1993 (24.06.93), column 1, line 27 - line 54; column 2, line 47 - line 68	1,3-6,8-10
Y		2,7
	--	
Y	US 5363448 A (P.J. KOOPMAN, JR. ET AL), 8 November 1994 (08.11.94), column 1, line 6 - line 10; column 2, line 47 - column 3, line 2	2,7
	--	
X	DE 4218500 A1 (TRW SIPEA S.P.A.), 10 December 1992 (10.12.92), column 1, line 64 - column 2, line 29; column 4, line 21 - line 41	1,3-6,8-10
	--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 October 1996	07 -10- 1996
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Anders Ströbeck Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NO 96/00117

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0636963 A2 (INTERNATIONAL BUSINESS MACHINES CORPORATION), 1 February 1995 (01.02.95), abstract ---	1,3-6,8-10
A	US 5351293 A (J.R. MICHENER ET AL), 27 Sept 1994 (27.09.94), abstract --- --------	1,3-6,8-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

05/09/96

International application No.
PCT/NO 96/00117

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE-A1- 4141766	24/06/93	NONE	
US-A- 5363448	08/11/94	CA-A- 2159360	12/01/95
		EP-A- 0706735	17/04/96
		WO-A- 9501685	12/01/95
DE-A1- 4218500	10/12/92	FR-A- 2678755	08/01/93
		GB-A,B- 2257552	13/01/93
		IT-B- 1249903	30/03/95
		JP-A- 8171404	02/07/96
EP-A2- 0636963	01/02/95	JP-A- 7107086	21/04/95
US-A- 5351293	27/09/94	NONE	